Theory - Ransomware part 2

In the previous section of the article, TipsMake.com introduced you to some basic information about Ransomware, CryptoLocker ... as well as how to operate, tap money of these fake software, spies. And this time, we will continue to dive into Ransomware as well as variants and relatives in the vast CryptoLocker family.

In the previous part of the article, TipsMake.com introduced you to some basic information about Ransomware, CryptoLocker . as well as how to operate, "tap money" of fake software, this spy . And this time, we will continue to dive into Ransomware as well as variants, "relatives" in the vast CryptoLocker family.

How to effectively prevent Ransomware

1. CryptoLocker data encryption method

Last time, TipsMake.com mentioned that **Ransomware** 's data encryption protocol is **RSA-2048** , but based on TrendMicro's analysis report, it is **AES + RSA** mechanism.

1. What is Part 1 of the Ransomware article?

If translated into English, **RSA** is asymmetric encryption. How to understand it right? This means that the encryption method will use up to 2 keys:

1. A key is used to encrypt data, the files that **CryptopLocker** finds (**public key**)
2. The other key is to decrypt encrypted (**private key**) files.

And also, this is how AES works. Types of malware often use the AES standard to encrypt user data and information. And there are also differences between **AES** and **RSA** here:

1. **The AES key** to decrypt the data is in the encrypted file itself.
2. **RSA Public Key** is in Malware itself, what does this mean? As a user will need to have a Private Key to decrypt the data.

More thorough studies and analyzes of many reputable security firms have shown that **CryptoLocker** does not work in a spontaneous manner, but has a specific Spam campaign included. More specifically, malicious files are included in the email users receive, often "promotion" of **TROJ_UPATRE** - a type of **Malware** , with extremely small capacity (only a few KB) with the function to download **ZBOT** to the computer. victims' properties. And then, these **ZBOTs** will continue to download and install the complete CryptoLocker.

Until the end of 2013, a new category of CryptoLocker appeared. It was **WORM_CRILOCK.A** - which could be spread through external storage devices such as USB Flash drives, external hard drives . (similar like **CRILOCK**). The difference of this type of malware is that they do not need to downloader or email attachments to spread to the victim's computer, but mainly they invade via **P2P** protocol (you often use, download files via Torrent will understand).

In addition, another Ransomware variant also appeared at this stage. It is a form of infection through email attachments, which are collectively known as **CryptoDefense** or **Cryptorbit** . Discovered by **TrendMicro** , this Ransomware strain is called **TROJ_CRYPTRBIT.H** , they are responsible for encrypting database files - database, web (file * .html), text file (Office), video file, audio, photo, text . or in short, any file other than * .msi or * .exe on the victim's computer. In addition, they "nibble" Windows backup and backup files to stop the Restore process.

2. The main purpose of CryptoLocker - Money

As mentioned in the target of the victim, **CryptoLocker** aimed and blackmailed the victim, and during this period hackers mainly targeted virtual currency - Bitcoin (which was storming at that time). More specifically, there are only two major variants of this type of malware, collectively called **BitCrypt:**

1. The first type: **TROJ_CRIBIT.A** encrypts all the data files it finds into a .bitcrypt file. Mainly used in English language.
2. The second type: **TROJ_CRIBIT.B is** similar to the above, but is different. It turns the victim's data into .bitcrypt 2, and uses many different languages ??(more than 10 types are detected).

Both of these Cribit types apply **RSA (426) -AES** and **RSA (1024) -AES algorithms** to encrypt information and data. Besides, there is still another type of Malware that is very terrible at this time, it is **FareIT** . **TSPY_FAREIT.BB** simply has the task of downloading Trojans to your computer, intruding and stealing personal data related to **wallet.dat** database **(Bitcoin)** , **electrum.dat (Electrum), and. wallet (MultiBit).** Why? Because those files contain personal data, information about currency transactions, accounts .

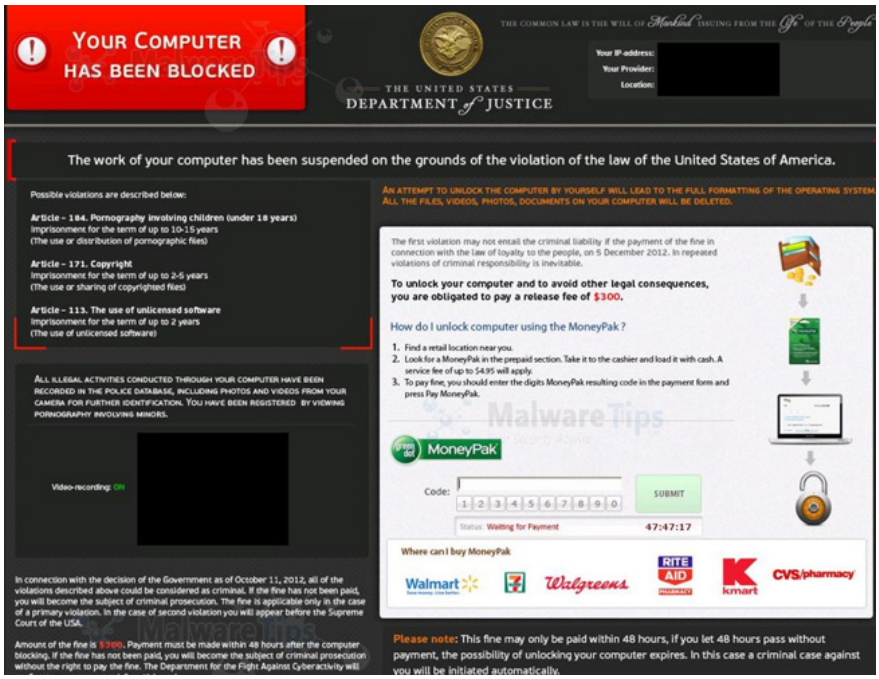
3. POSHCODER: PowerShell Abuse

As technology evolves, it is also when many features of the Windows operating system are exploited. This time is PowerShell on Microsoft's Windows platform.**TrendMicro** once again discovered **TROJ_POSHCODER** .A invades and **hijacks** PowerShell on the victim's computer. **PowerShell** only appears on Windows 7 (until Windows 10 - the latest version still exists), the main purpose of hackers when penetrating through **PowerShell** is to avoid detection of the system, the administrator (because **PowerShell** is a high-level Windows control tool).

Technically, **POSHCODER** uses the **AES** mechanism for data encryption, information, and **RSA Public key 4096** . And when all the files on the system are encrypted, the hacker will display a message:

4. Ransomware continues to view important files

When the Ransomware species are becoming more and more popular (in a sense), this does not mean that other less-known Ransomware strains have disappeared, but they simply hide themselves waiting for the opportunity to:



What made Ransomware different from their brothers and relatives? The answer is that the Vector versions of Ransomware are replaced by one other malicious Malware - collectively called Patched Malware. Understanding is the "patching" of Malware after being modified and infecting users' computers through the installation of add-

ons to the browser, downloading downloader files, attachments from email . with malicious code. Based on the frequency of using computer file types, hackers can easily determine the purpose, the important system files they are targeting (for example, if you regularly play games, browse the Internet, then hackers will create suitable patch files and files for those game files and browsers).

Another way to attack a victim's computer is to infiltrate directly into the **user32.DLL** file *(located in the* **c: WindowsSystem32** *folder).* Similar to how **PowerShell** attacks, this is considered a hacker self-defense method, because once a successful entry into these important files, the system will have no way of detecting the existence. in of malware.

5. What is the future for Ransomware

Before proceeding, please take a look at the "demonstration" video of TorrentLocker's operating process - a form of Ransomware that appeared in 2014:

The table lists the famous "members" in the Ransomware family:

Name Security **Alias Description** ACCDFISA Security Agency Ransom Internet Security Agency Ransom Discovered in early 2012, encrypted data file with a password. Ask users to pay via Moneypak, Paysafe, or Ukash. Resides as self-extracting files (* .SFX), often associated with applications like Sdelete and WinRAR. ANDROIDOS_LOCKER Considered the first Ransomware to appear on mobile platforms. Use TOR, anonymous services to connect. CRIBIT BitCrypt Similar to CRILOCK, they use RSA - AES to encrypt data. Version 1 uses RSA-426, while Version 2 uses RSA-1024. CRILOCK CryptoLocker Implement Domain Generation Algorithm (DGA) to make connections to C&C servers. Discovered in 2013, UPATRE hides in spam emails, secretly downloads ZBOT to a computer, and then turns to CRILOCK. CRITOLOCK Cryptographic locker Using high-end encryption standard AES-128, the word "Cryptolocker" will appear in Wallpaper images on the victim's computer. CRYPAURA Encrypt the file based on the email address it finds. CRYPCTB Critroni, CTB Locker, Curve-Tor-Bitcoin Locker Encrypt data files, delete system backup files for users to not back up or restore. Spread through spam emails, which contain attachments * .exe (downloader). Powerful spread through social networking. CRYPDEF CryptoDefense Encrypt personal information and data. Ask victims to pay ransom with Bitcoin. CRYPTCOIN CoinVault Similar to CRYPDEF, but there is an option for victims to decrypt any data file (only one file)! CRYPTFILE Using certain Public keys to create RSA-2048 encryption mechanism, the average price given to the victim is 1 Bitcoin for a decryption key. CRYPWALL CryptoWall, CryptWall, CryptoWall 3.0 Considered CRYPTODEFENSE updates, asking victims to transfer using Bitcoin, entering computers via spam emails, how to spread them with the UPATRE-ZBOT-RANSOM, CryptoWall 3.0 with Spyware FAREIT. CRYPTROLF Displays Troll photos after encrypting all user data. CRYPTTOR Change the victim's Wallpaper to a wall, then make a ransom request CRYPTOR batch file ransomware Spread through DOWNCRYPT VIRLOCK VirLock, VirRansom The main goal is text files, compressed files, media files (video, mp3, image .) PGPCODER Appeared in 2003, considered the "ancestor" of the first Ransomware KOLLAH One of the first Ransomware to use file encryption and change the file extension, target is Microsoft Office text files, PDF file KOVTER Form of attack through advertisements when users watch YouTube, the main goal is the security vulnerability Sweet Orange. MATSNU Backdoor has the ability to lock the system's screen, which is the entrance of Ransomware. ANSOM After entering the computer, it will prevent users from manipulating the system. Through it ransom! REVETON Police Ransom 64-bit VBUZKY Ransomware legal notice, other than the Shell_TrayWnd vulnerability, automatically activates the TESTSIGNING option on Windows 7. CRYPTOP Ransomware archiver Download GULCRYPT and other malware . GULCRYPT Ransomware archiver Encrypt files into other formats. CRYPWEB PHP ransomware

Very dangerous. Encrypt the database on the web server, causing the website to fall into: "Website unavailable". Use HTTPS protocol to connect to C&C server. CRYPDIRT Dirty Decrypt Appears before Cryptolocker. CRYPTORBIT Mainly infects image, text, HTML files containing the **Indicators Of Compromised (IOC).** CRYPTLOCK TorrentLocker Another name is CryptoLocker, which displays the **crypt0l0cker** message on the victim screen. CRYPFORT CryptoFortress Inherits TorrentLocker / CRYPTLOCK interface, relying on wildcards to find files in the file extension, encrypting files in shared folders. CRYPTESLA TeslaCrypt Similar to CryptoLocker, encrypting data files of Game, games. CRYPVAULT VaultCrypt Use GnuPG encryption tool, download malware hacked to user computers via browser, steal account information CRYPSHED Troldesh First discovered in Russia, add English in the period then, SYNOLOCK SynoLocker Exploiting Synology NAS vulnerability to encrypt data on that device. KRYPTOVOR Kriptovor

6. How to prevent Ransomware

Prevent:

In case your computer has the expressions described above, follow the steps below:

1. Turn off **System Restore (** see instructions for turning off System Restore on Windows 10 **)**
2. Use the **Anti Malware** program to Scan and delete suspicious files. (recommend AntiMalware of MalwareByte)

Prevent:

Because Ransomware is malicious software, it can appear and invade at any time. Therefore, we - computer users must pay attention to the following:

1. Back up important data regularly.
2. Update the software to the latest stable version.
3. Limit the use of crack, key (type * .exe) to unlock software.
4. Limit access to porn websites and black websites.
5. Do not click and download unknown sources via email.
6. Install and update regularly security programs, Internet Security format (currently sold a lot at META online supermarket). You can refer here, often with a discount program.
7. Trend Micro Maximum Security antivirus software 2015
8. Review security articles on website QuanTriMang.com or Fanpage TipsMake.com

7. Tactics against ransomware

Master File Table

The most special part of ransomware definitely comes from using encryption. But is that all? Engin Kirda, co-founder and chief architect at Lastline Labs, says that is not the case. He and his team (using research done by Amin Kharraz, one of the graduate students of Kirda) completed a massive ransomware study, analyzing 1359 samples from 15 ransomware families. The team's analysis explores the deletion mechanisms and finds some interesting results.

What are the delete mechanisms? About 36% of the 5 most common ransomware families in the dataset are deleting files. If you do not pay, the actual files will be deleted. In fact, file deletion is pretty simple.

How will a professional hacker do this? Hackers will aim to clean up the drive so that users will find it difficult to retrieve data. They will easily record or delete files from the drive. But most hackers are directly working on items in Master File Table and marking deleted items, but the data is still on the drive.

After that, deleted data can be retrieved and in many cases, fully recovered.

Family	Family Description				Types of Attacks			
	Samples	Variants	First Seen	Most Recent	Encypting Files	Changing MBR	Deleting Files	Stealing Info
Reveton	244(17.95%)	14	2012	2014			✓	✓
Cryptolocker	32 (2.35%)	4	2013	2014	✓			✓
CryptoWall	11(0.8)	2	2014	2014	✓			
Tobfy	122 (8.97%)	12	2010	2014			✓	
Seftad	23 (1.69%)	4	2006	2010		✓		
Winlock	308(22.66%)	27	2008	2013			✓	
Loktrom	4 (0.29%)	2	2012	2013				
Calelk	9 (0.663%)	2	2009	2010				
Urausy	523 (38.48%)	16	2009	2014			✓	✓
Krotten	17 (1.25%)	3	2008	2009				
BlueScreen	4 (0.29%)	1	2008	2009				
Kovter	8 (0.58%)	2	2013	2013				✓
Filecoder	9 (0.66%)	3	2012	2014	✓		✓	
GPcode	21 (1.54%)	4	2004	2008	✓			
Weelsof	24 (1.76%)	3	2012	2013				
No. of Samples	1,359	-	-	-	73(5.37%)	23(1.69%)	484(35.61%)	44(3.23%)
No. of Variants	-	99	-	-	13(13.13%)	4(4.04%)	29(21.33%)	6(6.06%)

Desktop environment

Another behavior ransomware usually does is lock the desktop. This type of attack is present in more basic variants. Instead of actually starting with encrypting and deleting files and ransomware that lock the desktop, users cannot manipulate the device. Most users consider this to mean that their files have disappeared (encrypted or completely deleted), then simply cannot be recovered.

Blackmail message

Ransomware will often ask the victim to pay a ransom. It usually requires users to pay a sum of money to get their files back safely. In addition, ransomware software developers take users to specific websites while disabling some system features - so they cannot get rid of that page / image. This is similar to a locked desktop environment. But it does not mean that the user files are encrypted or deleted.

8. Think carefully before you pay

Ransomware infection can affect many things. This is no doubt. However, the ransomware attack does not mean that your data will disappear forever. Hackers who develop ransomware are not great programmers. There is no reason to choose to become a hacker instead of a genuine programmer. In many cases, some users will pay for safety reasons. That is completely understandable.

Methods to minimize ransomware's ability to attack such as backing up regular files to an offline network drive, updating antivirus software and Internet browsing, watching phishing emails and being vigilant in downloading files from the Internet. For details, read the article: If you don't want to be a victim of Ransomware, read this article.

Hopefully, the above information has helped you partly understand Ransomware's operating mechanism, spyware, extortion software. In the next part of the article, TipsMake.com will introduce notes about variations

and relatives of Ransomware in recent years, how to prevent, prevent and handle when computers are infected with Ransomware.

Good luck!

See more:

1. 5 biggest ransomware attacks in the last 5 years
2. Summary of effective Anti-Ransomware software
3. 7 kinds of ransomware you didn't expect